

- [78] A. Romano, D. Lehmann, M. Pradel, and W. Wang, “Wobfuscator: Obfuscating JavaScript Malware via Opportunistic Translation to WebAssembly,” in *2022 IEEE Symposium on Security and Privacy (SP) (SP)*, (Los Alamitos, CA, USA), pp. 1101–1116, IEEE Computer Society, may 2022.
- [79] M. T. Aga and T. M. Austin, “Smokestack: Thwarting DOP Attacks with Runtime Stack Layout Randomization,” in *IEEE/ACM International Symposium on Code Generation and Optimization, CGO*, pp. 26–36, 2019.
- [80] S. Lee, H. Kang, J. Jang, and B. B. Kang, “SaVioR: Thwarting Stack-based Memory Safety Violations by Randomizing Stack Layout,” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 4, pp. 2559–2575, 2022.
- [81] Y. Younan, D. Pozza, F. Piessens, and W. Joosen, “Extended Protection against Stack Smashing Attacks without Performance Loss,” in *22nd Annual Computer Security Applications Conference (ACSAC 2006), 11-15 December 2006, Miami Beach, Florida, USA*, pp. 429–438, IEEE Computer Society, 2006.
- [82] Y. Xu, Y. Solihin, and X. Shen, “MERR: Improving Security of Persistent Memory Objects via Efficient Memory Exposure Reduction and Randomization,” in *ASPLOS ’20: Architectural Support for Programming Languages and Operating Systems*, pp. 987–1000, 2020.
- [83] G. S. Kc, A. D. Keromytis, and V. Prevelakis, “Countering Code-injection Attacks With Instruction-set Randomization,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS*, pp. 272–280, 2003.
- [84] E. G. Barrantes, D. H. Ackley, T. S. Palmer, D. Stefanovic, and D. D. Zovi, “Randomized Instruction Set Emulation to Disrupt Binary Code Injection Attacks,” in *Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS*, pp. 281–289, 2003.
- [85] M. Chew and D. Song, “Mitigating Buffer Overflows by Operating System Randomization,” Tech. Rep. CS-02-197, Carnegie Mellon University, 2002.
- [86] D. Couroussé, T. Barry, B. Robisson, P. Jaillon, O. Potin, and J. Lanet, “Runtime Code Polymorphism as a Protection Against Side Channel Attacks,” in *Proceedings of Information Security Theory and Practice - 10th IFIP WG 11.2 International Conference, WISTP*, vol. 9895, pp. 136–152, 2016.
- [87] M. Jacob, M. H. Jakubowski, P. Naldurg, C. W. Saw, and R. Venkatesan, “The Superdiversifier: Peephole Individualization for Software Protection,” in *Proceedings of Advances in Information and Computer Security, Third*

- International Workshop on Security, IWSEC 2008*, vol. 5312, pp. 100–120, 2008.
- [88] M. Henry, “Superoptimizer: A Look at the Smallest Program,” *ACM SIGARCH Computer Architecture News*, vol. 15, pp. 122–126, Nov 1987.
 - [89] V. Le, M. Afshari, and Z. Su, “Compiler Validation via Equivalence Modulo Inputs,” in *ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI*, pp. 216–226, 2014.
 - [90] B. R. Churchill, O. Padon, R. Sharma, and A. Aiken, “Semantic Program Alignment for Equivalence Checking,” in *Proceedings of the 40th ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI*, pp. 1027–1040, 2019.
 - [91] V. Le, M. Afshari, and Z. Su, “Compiler Validation via Equivalence Modulo Inputs,” in *ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI*, pp. 216–226, 2014.
 - [92] N. Harrand, C. Soto-Valero, M. Monperrus, and B. Baudry, “Java Decompiler Diversity and Its Application to Meta-decompilation,” *J. Syst. Softw.*, vol. 168, p. 110645, 2020.
 - [93] M. Zalewski, “American Fuzzy Lop,” 2017.
 - [94] K. Zhang, D. Wang, J. Xia, W. Y. Wang, and L. Li, “ALGO: Synthesizing Algorithmic Programs with Generated Oracle Verifiers,” *CoRR*, vol. abs/2305.14591, 2023.
 - [95] L. de Moura and N. Bjørner, “Z3: An Efficient SMT Solver,” in *Tools and Algorithms for the Construction and Analysis of Systems*, (Berlin, Heidelberg), pp. 337–340, 2008.
 - [96] A. Abate, C. David, P. Kesseli, D. Kroening, and E. Polgreen, “Counterexample Guided Inductive Synthesis Modulo Theories,” in *Proceedings of Computer Aided Verification - 30th International Conference, CAV*, vol. 10981, pp. 270–288, 2018.
 - [97] P. M. Phothilimthana, A. Thakur, R. Bodík, and D. Dhurjati, “Scaling up Superoptimization,” in *Proceedings of the Twenty-First International Conference on Architectural Support for Programming Languages and Operating Systems, ASPLOS*, pp. 297–310, 2016.
 - [98] R. El-Khalil and A. D. Keromytis, “Hydan: Hiding Information in Program Binaries,” in *Information and Communications Security, 6th International Conference, ICICS*, vol. 3269, pp. 187–199, 2004.